4/pkt

A METHOD FOR THE PROTECTED MANAGEMENT OF A UNIT COUNTER AND A SECURITY MODULE IMPLEMENTING THE METHOD

INSA1

The object of the present invention is a method for the protected management of a unit counter located in memory, in particular a chip card in relationship with a terminal. It could nevertheless apply to any other type of memory.

The invention is particularly useful when it is a case of counting a very large number of units whilst preserving the storage capacity of the memory.

The storage capability of the memory (its suitability for being updated) is limited in time because of the technology used by the manufacturers of

electrically erasable and programmable non-volatile memories (for example EEPROMs).

The manufacturers guarantee the good behaviour of the memory for a limited number of updates of the memory (an update comprises an erasure operation followed by a programming or writing). Beyond that, the memory may no longer be correctly erased or correctly programmed.

On average, the number of updates guaranteed by the memory manufacturers is around 100,000 per memory location. In the case of a unit counter, the problem consisting in preserving the storage capability of the said counter is all the more difficult to resolve ~~since~~ due to the ~~is~~ high the number of units to be counted and ~~is great~~ the high ~~the~~ frequency of updating of the counter.

The invention will be described in particular in the case of an application to a chip card in the field of cardphones.

It is known, in the field of chip cards, that a transaction between a terminal and an external electronic purse is organised around a security module (SM) comprising a microprocessor. The module is generally integrated into the terminal.

The role of a security module is particularly to ensure the verification of the authentication of the electronic purse cards external to the terminal. In the context of cardphones, the electronic purse chip card is a phone card (not reloadable), the terminal is a cardphone (or telephone box) and the security module

can itself for example be a chip card located in the terminal.

It should be noted that the set of commands of the component of the said security module is referred to as the "operating system".

The use of a security module makes it possible to give the operator of a cardphone the means of authenticating the phone cards which are inserted by the customers carrying the said phone cards. Thus fraudulent cards are rejected.

In addition to the authentication functions, the module proposes to the operator of a cardphone to manage, in a secure manner, a unit counter which records all the units consumed by the different holders of prepayment cards or phone cards during telephone communications made from the said cardphone.

This functionality opens the way to multioperator solutions where the issuer of phone cards (the operator) would not be the sole operator of the cardphone. For this purpose, provision is made for having, within the memory of the security module located in each cardphone, a unit counter dedicated to each operator.

Still in the context of cardphones, such a counter must be able to store 16 million units, which corresponds to a maximum number of telephone units able to be recorded at very highly frequented public places (such as airports) for measurements made over the average lifetime of the counters of a cardphone (approximately 3 years).

The updating of the said counter can also be required on several occasions during a telephone communication.

In order to store as many units using the counters of the prior art it would be necessary to use a 24-bit memory. However, in this case, the number of updates would exceed the storage capacity of this memory. This solution can therefore not be envisaged.

Summary of the Invention

In the invention, provision has been made for remedying this problem by breaking down the unit counter into at least two main areas.

The first memory area of the counter (zone A) is considered to be a bit field. A consumed communication unit corresponds to each bit stored or " blown" or "written" or "switched on". A "token" is also spoken of to characterise a bit stored in area A.

A second, smaller, memory area (area B), whose size makes it possible to code the maximum value of the number of units to be stored.

These memory areas are memory areas of an electrically programmable and electrically erasable non-volatile memory.

With regard to area A and without going into the technology of the programming of memories, a memory location will be considered to be unavailable when a bit is stored therein. Hereinafter the term stored bit or "switched-on bit" or "blown bit" or written bit will be used indifferently to mean that the memory locations are unavailable, and switched-off or not blown bit to mean that the locations are available (free).

By convention, it will be considered that a bit is switched on when its logic state is equal to 1, and that a bit is switched off when its logic state is equal to 0.

A switched-on bit will be made available (switched off) only at the next erasure of the entire area A (switching off of all the bits making it up).

The object of the invention is therefore more particularly a method for the protected management of a unit counter in an electrically programmable memory, according to which the number of units consumed by users is recorded by means of a counter, principally characterised in that it consists in breaking down the unit counter into at least two memory areas (A, B), a first area (A) in which at least one bit is stored per at least one consumed unit and a second area (B) in which the value corresponding to the total units consumed is stored, the second area being updated only when the number of units consumed exceeds or attains the number of not stored bits of the first area.

The units consumed are recorded in the first area cyclically.

A cycle corresponds to a sequence of switching on the first bit from the first area (A) to the last. It ends when all the bits have been switched on.

An operation of recording n units consumed comprises the following steps:

- reading the content of the first area and comparing the number of not stored bits with the number of consumed units to be recorded,

- if this number of not stored bits is greater than or equal to the number of units to be recorded, the bits to be recorded are stored in the said area,

- if this number is less, this number of bits is stored in the first area and the remaining units are recorded in the second area by performing an operation of updating this area, and the first area is erased.

An operation of updating the second area (B) comprises a step of writing in this second area a new coded counter value equal to the current value to which the number of not blown bits in the first area (A) and the remaining consumed units to be stored are added.

The updating of the second area comprises a prior step of recording indicator information meaning that an updating is taking place, then, when the updating is ended, the updating consists in erasing the first area (A) and erasing the indicator information.

To improve security the unit counter has an area (SB) for backing up the second area (B) and these two areas each have a field for recording a redundancy code (CR, SCR), for checking the integrity of the content of these two areas.

An operation of recording n units consumed also comprises a prior step of verifying the state of the counter comprising the following operations:

- verifying the absence of the indicator information for a current update:

- where the indicator information is indeed absent:

- verification of the validity of the fields containing the redundancy codes:
  - . where the fields are valid:
    - recording of the n units;
  - . where the fields are not valid:
    - detection of a fault and stoppage of the counter,
- where the indicator information is present:
  - activation of the recovery operation to re-establish the integrity of the contents of the counter.

An operation of updating the second area then includes the following steps:

- recording the indicator information,
- copying, in the backup area (SB) the coded value of the counter of the second area (B),
- recording the new coded value of the counter in the second area (B),
- erasing the first area (A),
- erasing the indicator information.

The recovery operation consists in determining at which step the abnormality occurred (a cutting off of the current), and then performing, according to the circumstances determined, the steps of updating the backup area (SB) and/or of the second area (B) and/or of the first area.

Advantageously, the determination of the step at which the abnormality occurred consists in reading the content of each of the areas in order to determine whether the abnormality occurred during the updating of the backup area (SB), case 1, during the updating of

the second area (B), case 2, during the erasure of the first area (A), case 3, between the updating of the second area (B) and the backup area (SB), case 4, or after the updating of these two areas, case 5.

In practical terms, the recovery consists in case 1 in :

- copying the value contained in the second area (B) into the backup area (SB),

- updating the second area (B) by recording the new value which is equal to the former one to which the content of the first area (A) is added,

- erasing the first area (A),

- erasing the indicator information (C2);

in case 2 in :

- copying into the second area (B) the value contained in the backup area (SB), adding the value contained in the first area (A),

- erasing the first area (A),

- erasing the indicator information (C2);

in case 3 in :

- erasing the content of the first area (A),

- erasing the indicator information (C2);

in case 4 in :

- implementing the steps according to case 2;

in case 5 in :

- implementing the steps according to case 3.

Advantageously the method also comprises a step of recording information signifying a failure in reading or writing to the first area (A) deactivating the said area when it has not been possible to read or write in

this area, and a step of reading this information at each new cycle, the units consumed then being directly recorded in a coded manner by an operation of updating the second area (B).

The information (C2) indicating a current updating and the information signifying a failure (C1) in reading and writing to the first area are recorded in a third area (C) of the said counter.

The invention also relates to a security module implementing the method according to the invention.

Such a module can be located in a terminal managing units consumed by the users of the terminal, and can also be in particular a telephony terminal.

Brief Description of the Drawing

Other particularities and advantages of the invention will emerge from a reading of the description below, which is given by way of non-limitative example with regard to the accompanying drawings, in which:

- Figure 1 schematically depicts the unit counter according to the invention;

- Figure 2A depicts the steps of recording n units according to the method of the invention;

- Figure 2B depicts the prior verification step 10 of Figure 2A;

- Figure 3 depicts the steps of recording the units in the second area (updating) according to a preferred embodiment;

- Figure 4 depicts the steps of the recovery mechanism;

- Figure 5 illustrates a variant in the according to the invention.

Detailed Description

The method described hereinafter relates to a counter protected against fraud (intrusion or tampering). The method provides, when the counter is saturated, for the latter to stop and informs the application using it of this fact.

In the example application given below, and which corresponds to the case of cardphones referred to in the introduction, the units consumed are telephone units and the sizes of areas A and B are obviously defined here for the purpose of example.

It is pertinent to consider an area A of 168 bits and an area B of 24 bits (24 bits in fact making it possible to store 16,777,215 units).

Area B is in turn split in order to overcome problems of cutting off of current during the updating of the counter (cf Figure 1). This case is detailed below.

As already mentioned, the operating life of the counter is directly related to the number of updates (erasure and writing). It is therefore essential to find a counter structure and a counting method which reduces the number of updates.

In the context of the invention, the storage of the communication units consumed takes place as follows.

It is assumed that the duration of a telephone communication is divided into time intervals. The duration of a time interval corresponds to a fixed number of consumed units. In this example, the

recording cycle for the consumed units is defined by these time interval.

At the start of each time range, the number of units consumed must be stored in the security module.

Thus, in the case of a communication requiring 13 units in total and where an elementary time interval comprises 3 units, the unit counter within the security module will be updated five times during the communication and a sixth time at the end of the communication time.

The method of managing the unit counter is defined by steps 10, 20, 30, 40, 50 and 60 illustrated by Figure 2A.

A step prior to the recording of the units consists in checking the state of the counter (step 10) detailed from Figure 2B.

At each request to store consumed units, the operating system of the security module managing the counter checks that the number of switched-off (available) bits in the area A is greater than or equal to the number of units to be stored (cf Figure 2A).

In the affirmative, if n units have been consumed, n bits available in the area A are blown (provision can be made, by way of a variant according to the invention, for n bits available in the area A to be blown for n packets of consumed units).

This operation requires no erasure and only one action of writing amounts to blowing certain bits in the area A.

As soon as the number n of consumed units to be stored exceeds the number of available bits L remaining in the area A, the number of available bits L in the area A are switched off and the remaining consumed units n-L are counted in the area B. A new coded value taking account of these remaining units is recorded in the area B by an updating operation as follows:

The new value of the area B (the total number of units) is equal to the current value of the area B to which it is necessary to add the number of bits blown in the area A (value VA) and the number n-L of units to be stored.

The updating of the area B gives rise to a reading thereof followed by an erasure and writing.

The area A for its part is entirely erased (all the bits are once again available).

It would also be possible, according to the invention, where the number of bits available in the area A is insufficient, to make provision for supplementing this area A, and then updating the area B by storing as a new value the previous value to which the content of the area A is added, and then erasing the area A and finally storing in the area A the remaining units consumed (instead of storing them in the area B). This variant does indeed remain within the scope of the principle of the invention.

With this method, although the frequency of storage of consumed units is high, the frequency of erasure of the areas A and B is much lower. The same applies to the frequency of writing to the different

memory locations making up the area A and consequently area B.

The frequency of erasing and writing to the memory locations making up the unit counter is directly related on the one hand to the size of the area A and on the other hand to the granularity used for breaking down a communication (granularity means an elementary communication period corresponding to a number of units predetermined by the operator).

It should be noted that, in order to know at any time the total number of units consumed by means of the cardphone, it suffices to add, to the current value of the area B, the number of blown bits in the area A.

In the context of the invention, it is proposed to use an additional functionality for extending the service life of the unit counter.

This is because it is known that a bit field is subdivided into sets of consecutive eight bits known as bytes. As is described above, the area A is erased as frequently as the area B. However, for programming facilities or constraints related to the component used, blowing a bit within a byte may give rise to a new blowing of bits already blown within the said byte.

Thus a byte belonging to the area A can be written to more often (that is to say its bits blown) than a byte making up the area B. The area A then being more stressed than the area B, the operating life of the counter is therefore directly related to the storage capacity of the area A.

To overcome this problem, it is proposed, in the context of the invention, to provide, within the unit counter, an additional memory area known as area C comprising at least one location for storing the information C1 (cf Figure 1 and Figure 5).

This variant of the method is illustrated by Figure 5.

In this variant, the step of verifying the state of the counter, prior to the recording of the consumed units, includes a reading of the area C in order to check whether the information C1 exists.

This information C1 is written as soon as a memory location in the area A can no longer be erased or written to (since provision is made in a conventional manner to check the correct execution of a writing or erasure in the memory). In this case the operating system of the security module decides to deactivate the area A (step 42) and to work only with the area B (step 80). With each request to store consumed units the area B is erased and rewritten.

Quite obviously, the storage capacity of the area B will in turn be rapidly impaired but the counter can continue to be used for some time more.

Moreover, in order to increase the security of the management of the counter, it is possible to add a mechanism for guaranteeing a coherent state of the said counter, if a cutting off of current occurs during the storage operation. It is not pertinent to envisage an operation of pulling out the security module since generally this is fully integrated into the cardphone.

Having said this, the case of pulling out would be managed in the same way.

In the context of the invention, in order to install such a mechanism (hereinafter referred to as a recovery mechanism), the area B is provided with a redundancy code. In addition the area B is duplicated (cf Figures 1, 2B and 3).

The area SB thus defined is used as a backup for the previous one. It is updated before any change to the area B.

The area SB contains at any time the value of the area B, preceding the last updating of the said area.

An additional byte within the area C is used to indicate whether the storage operation has been partially or entirely performed; this is the indicator information C2.

Thus, at the start of processing of a request to store units, C2 is stored. It is erased once this same storage operation has been fully carried out. To avoid excessively stressing the byte C2, the latter is used (written and then erased) only in the case where the number of units to be stored is greater than the number of bits still available in the area A.

If this is not the case, the byte C2 is unused. Amongst the available bits in the area A, n bits are switched on. The storage operation is terminated. It is considered that the loss of information is minimal.

Where the number of bits available within the area A is insufficient, it is essential to activate the

procedure making it possible subsequently to actuate the recovery mechanism where there is an abnormality.

This is because, if a cutting off of current occurs after the area B has been erased and not once again rewritten to, all the information in the unit counter would be lost.

The step prior to any recording of a check on the counter (Figure 2B) will now be detailed.

The system checks the absence of the indicator C2 (11).

If the indicator C2 is absent (12), the system checks the fields containing the redundancy codes.

If these fields are valid (13), the n units consumed are recorded.

If the fields are not valid (14), there is a detection of a fault, a stoppage of the counter (and possibly an alarm).

In the case where the indicator exists (15), there is a use of the recovery mechanism detailed from the figure.

The operation of updating the area B according to this variant (cf Figure 3) will now be detailed.

As can be seen in Figure 3 (steps 51 to 55), the indicator C2 is first of all written, and the current value, for example V0, of the counter coded in the area B is copied into the area SB. Then the area B is updated (new value V1 equal to the current value to which the number of bits blown in the area A and the n-L units remain to be stored are added). The area A is next erased and the indicator C2 is then erased to

indicate that the storage operation has been performed entirely with success.

In the description given, everything occurs normally, there has not been any cutting off of power during the storage operation.

Now, if a cutting off has occurred, the activation of the recovery mechanism is described below (cf Figure 4).

This is activated at the time of the next request to store whether or not the number of bits available within the area A is sufficient to store the n units.

If the indicator C2 is switched on, then, before storing the consumed units, the recovery mechanism is actuated by the operating system of the security module.

Several cases may occur. This is because the cutting off may have occurred during the updating of the area SB (case 1), during the updating of the area B (case 2), during the erasure of the area A (case 3) or between the said updatings (case 4 and case 5).

The recovery procedure must be distinct according to the different cases listed above.

Where the area SB has not been able to be correctly updated (case 1), the redundancy code SCR thereof is not in conformity. The value V0 contained in the area B is then copied into the area SB, the area B is then updated (new value V1 equal to the current value V0 of the area B to which it is necessary to add the number of blown bits in the area A, value VA).

Only the number of units n-L which were to be stored during the interrupted storage is lost.

The area A is then erased and the indicator C2 too.

In the case where the area SB has been correctly updated but the area B has not been correctly updated (case 2), the redundancy code SCR of the area SB is correct. On the other hand, the redundancy code CR of the area B is incorrect.

The area B is then updated as follows:

The new value V1 of the area B is equal to the value V0 of the area SB, to which the number of blown bits in the area A, that is to say a value VA, V1 = V0 + VA, is added.

In this case as in the previous one, the only information lost corresponds to the number n-L of units remaining which were to be stored during the interrupted storage. The area A is then erased and the indicator C2 too.

By examining only the redundancy codes of the area SB and of the area B, it is impossible to know whether the cutting off of current took place between the updating of the areas SB and B (case 4) or after the updating of these two areas (case 5). This is because in both cases the redundancy codes are both correct.

To distinguish cases 4 and 5, the operating system of the security module compares the values of the areas SB and B; V(SB) = V(B)?:

If the area SB contains the same value as the area B then the cutting off of the power must have taken

place between the updating of the areas SB and B (case 4). The treatment of the recovery mechanism is then identical to that described above (case 2).

If this is not the case, the area B must therefore have been correctly updated (case 5). It is then necessary to erase the area A and the indicator C2. No information has been lost in this case.

The case where the cutting off of current took place during the erasure of the area A (case 3) remains to be dealt with. This case is similar to the previous case (case 5).

Once the recovery mechanism has been executed, the n units to be stored are stored in accordance with the description of the invention given above.